

A horizontal dotted line in dark blue, starting from a solid dark blue square on the left and extending across the top of the slide.

# Phishing Problems: Technology and Countermeasures

Christoph Fischer  
cfischer@bfk.de  
BFK edv-consulting GmbH  
Karlsruhe, Germany

# Who am I?



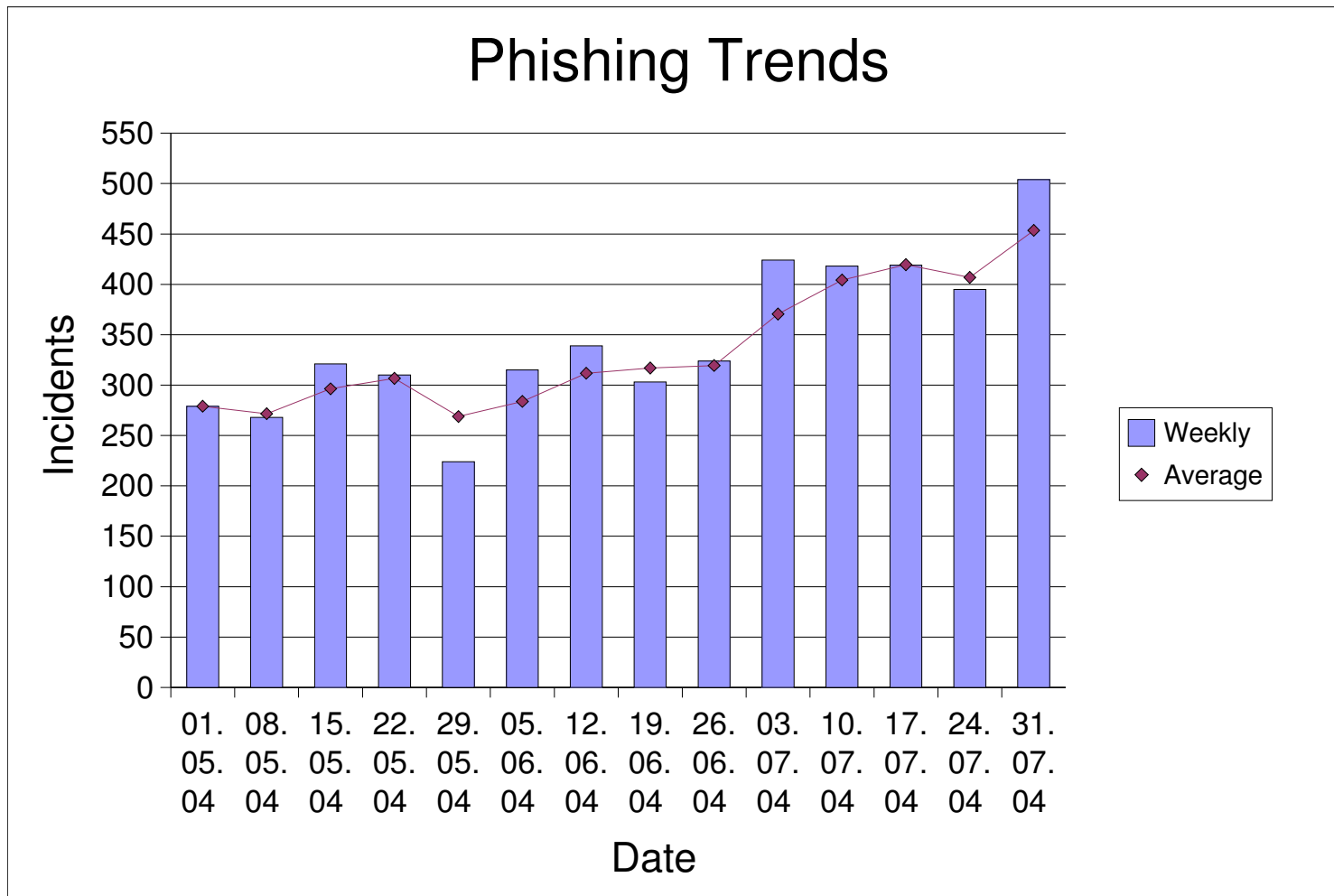
- Started IT security research at the University of Karlsruhe in 1987
- Founding member of CARO and Eicar
- First CERT in Germany
- First European FIRST Member
- Founded an IT security company in 1989/90
  - Preventive measures
  - Emergency Response / Forensics
  - Open Source Monitoring

# Why Anti-Phishing?



- In May we started a joint development with Cogenta Systems Ltd (London, UK)
- Presentation to a bank IT outsourcing company
- First incident the very next day
- No free weekend since then...

- Data based on anti-phishing.org



- The distribution changed over time
  - Early incidents targeted login credentials
  - Today banking is the prime target
  
- Distribution (anti-phishing.org)
  - 83% financial services
  - 13% e-commerce
  - 4% ISP

- Financial loss
  - Germany sofar no known losses
  - Australia: 200 million AUS\$ in 2003
  - US figures vary some quote over one billion
- Reputation
- Damage of acceptance of e-banking

# Stages of an Attack



## Preparations

Target selection

## Infrastructure

Creation of covert e-mail accounts

Domain reservation

## Attack

Fake web site deployment

SPAM mailing

## Harvest

Identity misuse

multiple international funds transfers

withdrawal

# Sample SPAM



Sehr geehrter Postbankkunde,

In der letzten Zeit ist es sehr häufig zu betrügerischen Vorfällen bei unserem Service gekommen! Verschiedenste Spion-Programme installieren sich unbemerkt auf Computern unserer Kunden und verwenden persönliche Daten als Betrüger!

Um sich dagegen zu schützen empfehlen wir Ihnen die neuesten Antivirusprogramme zu installieren und diese täglich zu erneuern!

AntiVir Personal Edition  
[www.fox-it.de](http://www.fox-it.de)

Trotz allem haben unsere Experten ermittelt, dass in etwa jedem zweiten Rechner ein Trojaner steckt und die Passwörter der Postbank auch weitergeschickt wurden!

Um dieses Problem zu lösen wollten wir jeden einzelnen Kunden erneut identifizieren um so die Betrüger zu stoppen! Mit diesem Verfahren erreichen wir Ihnen die höchste Sicherheit zu bieten! Die Identifizierung wird durch den Mail so können wir Sie in Zukunft identifizieren und nur Sie werden Zugriff auf Ihr Konto haben!

Bitte loggen Sie sich jetzt in Ihr Konto ein (die Einwahl soll unbedingt von zu Hause erfolgen)

<http://www.postbank.de>

Vielen Dank für Ihr Verständnis und Ihre Mitarbeit

© 2004 Deutsche Postbank AG  
[www.postbank.de](http://www.postbank.de)

# Sample Page

The screenshot displays the Postbank website interface. At the top, there is a navigation bar with links for 'Startseite', 'Kontakt', 'Der Bank', and 'Hilfe'. Below this, a search bar is visible. The main content area is divided into several sections:

- Navigation:** A vertical yellow sidebar on the left contains various service categories such as 'Produkte & Preise', 'Service & Hilfe', 'Anfragen & Support', 'Easytrade', 'Versichern & Vermögen', 'Baufinanzierung', 'Online-Services', 'Mobile Services', 'Vermögensübertragung', 'Markt & Research', 'Presse', 'Investor Relations', 'Wir über uns', and 'Karriere'.
- Account Types:** A horizontal menu at the top right identifies 'Privatkunden', 'Geschäftskunden', and 'Firmenkunden'.
- Login Section:** A central area titled 'Log in' contains input fields for 'Postbankname', 'PIN', 'TAN', and 'Funktion' (with a dropdown menu set to 'Kontostand'). A 'Log in' button is located at the bottom of this section.
- Account Information:** A box on the right side displays account details: 'Kontostanz', 'Sie kennen unser Online-Banking noch nicht? Dann testen Sie selbst.', 'Kontonummer: 9 999 999 999', 'PIN: 11111', and 'TAN: 111111'.
- Promotional Banners:** Several banners are present, including one for 'Sicherheitskonzept des Online-Banking' with the headline 'Überzeugende Argumente gegen gezieltes Misstrauen!', another for 'Jetzt Bonus-Chance nutzen!', and one for 'Postbank Privatkredit' offering a '6,80% p.a.' interest rate.
- Quickfinder:** A search box at the bottom right is labeled 'Quickfinder' and contains the text 'Bitte wählen Sie aus'.

# First five cases in Germany

Financial Institution	Domain reservation date	Mail account creation date	SPAM mailout	Detection Date	Phishing stopped date	comment
Group (1)	2004/05/20 17:23Z DE	DE				
Group (2)	2004/05/30  FL, USA/ CAN	IL				
Bank 1	2004/06/20 FL, USA / CAN	IL	?	2004/06/24 Ca 07:00Z	2004/06/24 17:40Z	
Bank 2	2004/06/30 00:00Z CA, USA	?	2004/07/03 19:10Z GA, USA		2004/07/05 15:59Z	
Bankgroup	2004/06/30 06:44Z GA, USA	IL				Domain was reserved, no content

- Group 1
  - ◆ Very good German skills
  - ◆ Fixed Hosting
  - ◆ SPAM via hosting server
  - ◆ transport of ' harvest' via e-mail
- Group 2
  - ◆ Very bad German and English
  - ◆ Cyrillic tags in mail
  - ◆ Injected Hosting on privat PCs
  - ◆ SPAM via BOT
  - ◆ transport of ' harvest' via e-mail

- Group 3
  - ◆ Not real phishing
  - ◆ Fixed hosting on IIS
  - ◆ 419 / Nigeria Scam
  
- Group 4
  - ◆ Very bad German and English
  - ◆ Trojan horse
  - ◆ Distribution via SPAM
  - ◆ very universal concept
  - ◆ chinese language skill

# 'learning curve' of the attackers



May 2004:

- Input forms accept any data
- Domain registration and harvesting via same e-mail address
- DE domain and hosting in Germany

April 2004:

- Account numbers were tested for consistency

June 2004

- Multiple e-mail addresses were used

# 'learning curve' of the attackers



June 2004

- Pop-Up in Kiosk-Mode and redirect of the main page to the legitimate page of the bank

July 2004

- Hosting in difficult to reach countries (timezone, language)

September 2004

- Multiple hosting sites in one attack

# Technical traces

- Artefacts in the internet
  - Domain names, information clutter
- SPAM
  - Honeypots
- Web
  - Referrer logs
- Mail
  - Bounces

- PR
  - News flash on web
  - Press release
- Awareness
  - Prevention for cutomers
  - Staff training
- Ad hoc measures
  - Script injection
  - Logo swap
  - Change of variable naming

- [www.anti-phishing.org](http://www.anti-phishing.org)
- [www.usdoj.gov/ag.speeches/2004/82604ag.htm](http://www.usdoj.gov/ag.speeches/2004/82604ag.htm)
- [www.bankenverlag.de](http://www.bankenverlag.de)

# Contact



BFK edv-consulting GmbH

Durlacher Allee 47

76131 Karlsruhe

+49 721 9 62 01-1 tel

+49 721 9 62 01-99 fax

[info@bfk.de](mailto:info@bfk.de)

[www.bfk.de](http://www.bfk.de)